ABSTRACT

The invention provides a method and apparatus for transmitting data securely using an unreliable communication protocol, such as User Datagram Protocol. In one variation, the invention retains compatibility with conventional Secure Sockets Layer (SSL) and SOCKS protocols, such that secure UDP datagrams can be transmitted between a proxy server and a client computer in a manner analogous to conventional SOCKS processing. In contrast to conventional SSL processing, which relies on a guaranteed delivery service such as TCP and encrypts successive data records with reference to a previously-transmitted data record, encryption is performed using a nonce that is embedded in each transmitted data record. This nonce acts both as an initialization vector for encryption/decryption of the record, and as a unique identifier to authenticate the record. Because decryption of any particular record does not rely on receipt of a previously received data record, the scheme will operate over an unreliable communication protocol. The system and method allows secure packet transmission to be provided with a minimum amount of overhead. Further, the invention provides a network arrangement that employs a cache having copies distributed among a plurality of different locations. SSL/TLS session information for a session with each of the proxy servers is stored in the cache so that it is accessible to at least one other proxy server. Using this arrangement, when a client computer switches from a connection with a first proxy server to a connection with a second proxy server, the second proxy server can retrieve SSL/TLS session information from the cache corresponding to the SSL/TLS communication session between the client device and the first proxy server. The second proxy server can then use the retrieved SSL/TLS session information to accept a session with the client device.